Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Protection Profile (PP)

Application date/ID	2009-11-4 (ITC-9276)
Certification No.	C0247
Sponsor	Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan
Name of PP	Protection Profile for ePassport IC with Active Authentication
Version of PP	1.00
PP Conformance	None
Assurance Package	EAL4 Augmented with ALC_DVS.2, AVA_VAN.5
Developer	Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan
Evaluation Facility	Evaluation Center, Electronic Commerce Security Technology Laboratory Inc.

This is to report that the evaluation result for the above PP is certified as follows.
2010-2-25

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center

Evaluation Criteria, etc.: This PP is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 3
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3

Evaluation Result: Pass
"Protection Profile for ePassport IC with Active Authentication – Version 1.00" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Protection Profile for ePassport IC with Active Authentication, Version 1.00" (hereinafter referred to as "the PP [1]") developed by Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan, and evaluation of the PP was finished on 2010-2-25 by Evaluation Center, Electronic Commerce Security Technology Laboratory Inc. (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan and provides information to the procurers and developers who are interested in this PP.

The reader of the Certification Report is advised to read the PP that is the appendix of this report together. The operational conditions, details of usage assumptions, corresponding security objectives, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the PP.

This certification report assumes "vender who develops and supplies the ePassport IC corresponding to Active Authentication" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee individual IT product itself.

1.1.1 Assurance Package (EAL)

Assurance Package of the TOE is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

1.1.2 PP Conformance

There is no PP to be conformed.

1.2 Evaluated PP

1.2.1 PP Identification

The identification of this PP is as follows:

Name of PP:	Protection Profile for ePassport IC with Active Authentication
Version:	1.00
Developer:	Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan

1.2.2 Product Overview

This PP defines the specification of security requirements for ePassport IC interfiled in the passport, in accordance with the guidelines provided by the International Civil Aviation Organization (ICAO).

PP or ST that claims conformance to this PP shall claim exact conformance.

In this PP, the term "TOE" is defined as ePassport IC (including necessary software). This ePassport IC is composed of IC chip hardware with the contactless communication interface, basic software (operating system) that is installed in the said hardware and ePassport application program. The hardware has a contactless communication antenna externally connected thereto and is embedded in the plastic sheet together with the antenna to constitute part of passport booklet.

The TOE life cycle has four phases. Phase 1 is a "Development phase", in which IC chip hardware, basic software (e.g. operating system), etc. are developed. Phase 2 is a "Manufacturing phase", in which IC chip is manufactured and embedded with antenna in the plastic sheet. Phase 3 is a "Personalization" phase, in which a passport booklet is produced and personal data are written by the passport issuing authorities. Phase 4 is an "Operational Use phase", in which the TOE is used by the passport user, i.e., the passport holder in operational environment. In Phase 4, at immigration, the passport is inspected using a passport inspection terminal (hereinafter referred to as the "terminal"). Information printed on the passport booklet in ordinary characters are encoded in the same contents, printed in the machine readable zone (MRZ) of the passport booklet, and read by the optical character reader of the terminal. In addition, the information is digitized and stored on the IC chip, i.e., the TOE. These digitalized data are read from the terminal through the contactless communication interface of the TOE.

In Phase 1 and Phase 2, threats to the operational environment are not assumed, but proper development security shall be maintained to protect the confidentiality and integrity of configuration items of data developed and IC chips. In Phase 3, no explicit attack against the TOE is assumed, but security functionality that allows only an individual having authority to process the TOE is required. In Phase 4, security functionality that can counter attacks from attackers having a high attack potential is required.

The main security functions of the TOE are designed to protect data stored in the TOE in Phase 3 and Phase 4 from illicit reading or writing. The operation of the security functions applying to contactless communication with the terminal shall comply with the Basic

Access Control and Active Authentication Standards prescribed by the ICAO Doc 9303, Part 1 [14], [15]. Further, since attacks against protected data in the TOE are assumed to be those through the contactless communication interface of the TOE and those attempting to disclose internal confidential information through a physical attack against the TOE, the TOE shall have the security function of countering the said attacks. In addition, the TOE shall have the security function of controlling access to information in the TOE so as to enable only the authorized personnel to gain access to the information therein.

1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

The evaluation facility evaluated if the TOE is satisfied both Annex A of CC Part 1 (either of [5] or [8]) and Functional Requirements of CC Part 2 (either of [6] or [9]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7] or [10]) as its rationale. Such evaluation procedure and its result are presented in "Protection Profile for ePassport IC with Active Authentication, Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [13]. Further, evaluation methodology shall comply with the CEM (either of [11] or [12]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Reports prepared by Evaluation Facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification oversight reviews are also prepared for those concerns found in the certification process.

Those concerns pointed out by the Certification Body are fully resolved, and the Certification Body confirmed that the PP evaluation is appropriately conducted in accordance with CC ([5][6][7] or [8][9][10]) and CEM (either of [11][12]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and concluded fully certification activities.

2. Security Policy

2.1 Security Problems and Assumptions

Security Problems to be solved by the TOE conforming to this PP and assumptions required are as follows:

2.1.1.Threats

The TOE conforming to this PP shall assume threats listed in Table 2-1 and provide functions to counter them.

Table 2-1 Assumed Threats

Identifier	Threat
T.Copy	An attacker trying to forge the ePassport may forge the ePassport by reading personal information with digital signature from the TOE and writing the reproduced data in an IC chip having the same functionality as that of the TOE. This attack results in damage to credit for the whole Passport Booklet including the TOE.
T.Logical_Attack	In the operational environment after TOE embedded Passport Booklet is issued, an attacker being in a situation to read the MRZ data of the Passport Booklet may try to read confidential information (active authentication private key) stored in the TOE through the contactless communication interface of the TOE.
T.Physical_Attack	In the operational environment after TOE embedded Passport Booklet is issued, an attacker may try to disclose confidential information (active authentication private key) stored in the TOE by physical means. This physical means includes both of nondestructive attacks made without impairing the TOE functions and destructive attacks made by destructing part of the TOE to have physical access to the inside of the TOE.

2.1.2 Organizational Security Policies

Table 2-2 lists organizational security policies required for the use of the TOE conforming to this PP.

Table 2-2 Organizational Security Policies

Identifier	Organizational Security Policy
P.BAC	In the operational environment after TOE embedded Passport Booklet is issued, the TOE allows the terminal to read the given information from the TOE in accordance with the basic access control procedure prescribed by ICAO Doc 9303 Part 1. This basic access control procedure includes mutual authentication between the TOE and the terminals and secure messaging between the same. TOE files to be read are EF.DG1, EF.DG2, EF.DG13, EF.DG15, EF.COM, and EF.SOD under the standards stated above. About a file in the said standards other than the above, for any files that are not listed in this PP, the handling thereof is not defined. Any users other than the TOE are unable to have access to the basic access key file and the private key file that have stored internal TOE data.
P.Authority	The TOE under the control of the passport issuing authorities allows only authorized users (persons who succeeded in readout key, transport key, or active authentication information access key verification) to have access to the internal TOE data, as shown in Table 2-2-1.
P.Data_Lock	When the TOE detects a failure in authentication with the transport key, readout key or active authentication information access key, it will permanently invalidate authentication related to each key, thereby inhibiting reading or writing the file based on successful authentication thereof. Table 2-2-1 shows the relationship between the key used for authentication and its corresponding file in the TOE.
P.Prohibit	Any and all writing to the files in the TOE and reading

	from the files in the TOE based on successful authentication with readout key are inhibited after issuing the TOE to the passport holder. As the means, authentication invalidation through authentication failure with the transport key, readout key, and active authentication information access key (see P.Data_Lock) shall be used.

Note: P.Prohibit is a policy that inhibits EF.DG13 and EF.DG15 from being read through successful authentication using the readout key. Readout of EF.DG13 and EF.DG15 in the operational environment after the passport is issued is achieved by P.BAC.

Table 2-2-1 Internal TOE data access management by passport issuing authorities

Authentication status	File subject to access control	Operation permitted	Reference: Data subject to operation
Successful verification with readout key	EF.DG13	Read	IC chip serial number
	EF.DG15		Active authentication public key
Successful verification with transport key	Transport key file	Write	Transport key data
	Basic access key file		Basic access control encryption key Authenticator generation key
	EF.DG1		MRZ data
	EF.DG2		Facial image
	EF.DG13		Management data (Passport number and Booklet management number)
	EF.COM		Common information on basic coding rules
	EF.SOD		Security data related to passive authentication prescribed by ICAO Doc 9303 Part 1, Section IV, NORMATIVE APPENDIX 3
Successful verification with active authentication	EF.DG15	Write	Active authentication public key
	Private key file		Active authentication private key

information access key			

2.1.3 Assumptions for Operational Environment

Table 2-3 lists assumptions required in environment to use the TOE conforming to this PP.

The effective performances of the security functions of the TOE conforming to this PP are not assured unless the said assumptions are satisfied.

Table 2-3 Assumptions for Use of the TOE

Identifier	Assumption
A.Administrative_Env	The TOE that was delivered from the TOE manufacturer to the passport issuing authorities and is under the control of the authorities is subjected to the secure management and the issuing procedures until it is issued to the passport holder.
A.PKI	In order for the passport inspection authorities of the receiving state or organization to verify the authenticity of information that has been digitally signed by the passport Issuer and stored in the TOE (including the active authentication public key), the interoperability of the PKI environment both of the issuing and receiving states or organizations of the passport is maintained.

2.2 Security Objectives

The TOE conforming to this PP shall, as set forth below, counter threats defined in paragraph 2.1.1 and fulfill the organizational security objectives defined in paragraph 2.1.2 with the provided security functionalities.

(1) Security function to counter the threat "T.Copy"
This threat assumes that credit for the whole Passport Booklet including the TOE is damaged by reproducing information retrieved from the authorized IC chip in an illicit IC chip.

The TOE provides the active authentication function prescribed by the ICAO Doc 9303, Part 1. This embeds data that can verify the authenticity of the IC chip itself and allows the TOE to detect illicit IC chips and prevent the forgery of passport booklet.

(2) Security function to counter the threat "T.Logical_Attack"
This threat assumes that the active authentication private key leaks through the contactless communication interface of the TOE.

The TOE provides the function of inhibiting access to the active authentication private key through the contactless communication interface, and this prevents the active authentication private key from leaking.

(3) Security function to counter the threat "T.Physical_Attack"
This threat assumes that the active authentication private key leaks through a physical attack against the TOE.

The TOE provides the function of countering the following attack scenarios, and this prevents the active authentication private key from leaking:

- The attack discloses the active authentication private key by destroying the shell of the TOE and analyzing the TOE behavior through physical probing or manipulation to the internal circuit.

- The attack discloses the active authentication private key by interfering with the normal operation of the TOE through adding environmental stress (e.g. temperature, power supply voltage, clock application, electromagnetic pulse application, or light irradiation outside the normal operation range) to the TOE in operation and analyzing the behavior of the TOE at that time.

- The attack analyses the TOE behavior by monitoring electromagnetic waves leaking from the TOE in operation to disclose the active authentication private key.

(4) Security function to fulfill the organizational security objective "P.BAC"
This organizational security objective defines that the terminal shall securely read information from the TOE in accordance with the basic access control procedure prescribed by the ICAO Doc 9303, Part 1.

The TOE provides the basic access control function prescribed by the ICAO Doc 9303, Part 1, and this enables secure communication between the terminal and the TOE.

(5) Security function to fulfill the organizational security objective "P.Authority"
This organizational security objective defines for the TOE under the control of the passport issuing authorities that only authorized users can have access to the file in the TOE.

The TOE provides the function of making a request for authentication with the transport key, readout key, or active authentication information access key prior to having access to a file in the TOE and permitting access to the file in the TOE according to the authentication of the relevant key only in case of successful authentication, and this allows only authorized users to have access to the file in the TOE.

(6) Security function to fulfill the organizational security objective "P.Data_Lock"
This organizational security objective defines for the TOE under the control of the passport issuing authorities that, when the TOE detects a failure in authentication with the transport key, readout key or active authentication information access key, it shall inhibit reading or writing the file in the TOE based on the authentication with the relevant key.

TOE provides the function of permanently invalidating authentication related to each key with the transport key, readout key or active authentication information access key when it detects a failure in authentication with the relevant key, and this makes it possible to inhibit reading or writing the file in the TOE based on the authentication with the key.

(7) Security function to fulfill the organizational security objective "P.Prohibit"
This organizational security objective defines that writing to the file in the TOE and reading the file therein based on authentication with readout key are inhibited after issuing the TOE to the passport holder.

The TOE provides the function set forth in the preceding item (6), and this makes it possible to inhibit writing to the file in the TOE and reading the file therein based on authentication with readout key by intentionally causing an authentication failure with the transport key, readout key, or active authentication information access key prior to issuing the passport to the passport holder.

3. Evaluation conducted by Evaluation Facility and results Evaluation Result

3.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance components in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. In the Evaluation Technical Report, it explains the summary of the TOE, the content of evaluation and verdict of each work unit.

3.2 Overview of Evaluation Activity

The history of evaluation conducted was present in the Evaluation Technical Report as follows;

Evaluation has started on 2009-11 and concluded by completion the Evaluation Technical Report dated 2010-2. The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to the developer. These concerns were reviewed by the developer and all concerns were solved eventually.

Concerns that the Certification Body found about the evaluation process was described as a certification oversight review, and it was sent to Evaluation Facility. After Evaluation Facility and the developer examine it, these concerns were reflected in the evaluation report.

3.3 Evaluation Result

3.3.1 Evaluation Result

The evaluator determined with the Evaluation Technical Report that this PP fulfilled all work units prescribed in CEM.
As a result of the evaluation, the assurance components APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1, and APE_REQ.2 were determined as "PASS".

3.3.2 Comments/Recommendations of Evaluator

None

4. Certification

The certification body conducted the following certification based on each materials submitted by Evaluation Facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.

2. Contents pointed out in the Observation Report shall properly be reflected.

3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.

4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in certification process were prepared as certification oversight reviews and were sent to Evaluation Facility.

The Certification Body confirmed such concerns pointed out in Observation Report and certification oversight reviews were solved in the PP and the Evaluation Technical Report and issued this certification report.

5. Conclusion

5.1 Certification Result

As a result of verification of submitted Evaluation Technical Report, Observation Reports and related evaluation deliverables, Certification Body determined that the TOE satisfies all components of the EAL4 and components APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1 and APE_REQ.2 in the CC part 3.

5.2 Recommendations

There is no note.

6. Glossary

The abbreviations relating to CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

The abbreviations relating to PP used in this report are listed below.

ICAO	International Civil Aviation Organization
MRZ	Machine Readable Zone

The definition of terms used in this report is listed below.

ICAO Doc 9302	The following two documents are collectively referred to as the "ICAO Doc 9303, Part 1".
Part 1:	ICAO Doc9303 Machine Readable Travel Documents Part 1: Machine Readable Passports Sixth Edition, Volume 1 and 2; and SUPPLEMENT to Doc9303, Part 1, Sixth Edition, Release 7.
MRZ:	A machine readable zone, which consists of a digitalized facial image printed on the personal data page of ePassport and 88 letters provided at the bottom of the personal data page, in which the Name, Nationality, Sex, Date of birth, Passport No., Date of expiry, etc. of the passport holder.
National Printing Bureau:	An organization, which manufactures passport booklets and configures basic data (e.g. management data such as passport number, and active authentication public key and private key pair) to the TOE.
Passive authentication:	Security mechanism, by which the digital signature of the passport issuing authority is put on personal information data stored in the TOE, and the authenticity of data read from the TOE is verified by using the PKI system with assured interoperability both on the passport issuing and receiving

	sides. The passive authentication procedure has been standardized by ICAO.
Active authentication:	Security mechanism, by which the public key and private key pair based on the public key encryption system is stored and the private key is kept secret in the IC chip that is a part of the TOE. The public key is delivered to an external device trying to authenticate the TOE and the TOE is authenticated through cryptographic calculation by the challenge-response protocol using the private key, which has been kept secret in the TOE. The active authentication procedure has been standardized by ICAO.
Passport:	An identification document, which is issued by a national government or an equivalent public institution to an overseas traveler. The passport is normally issued in one-book form (passport booklet).
Passport office:	An organization, which configures the personal information of the passport holder to the passport booklet including the TOE and issues the passport. The passport office is set up in various regions and serves as contact to deliver the passport to the passport holder.
Passport issuing authorities:	In Japan, the National Printing Bureau and regional passport offices fall under the authorities.

7. Bibliography

[1] Protection Profile for ePassport IC with Active Authentication, Version number: 1.00 (February 15, 2010)

[2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 3 July 2009 CCMB-2009-07-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 3, July 2009, CCMB-2009-07-001 (Japanese Version 1.0, December 2009)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 3, July 2009, CCMB-2009-07-002 (Japanese Version 1.0, December 2009)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 3, July 2009, CCMB-2009-07-003 (Japanese Version 1.0, December 2009)

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[12] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004 (Japanese Version 2.0, March 2008)

[13] Protection Profile for ePassport IC with Active Authentication, Evaluation Technical Report Version 1.03 February19, 2010, Evaluation Center, Electronic Commerce Security Technology Laboratory Inc.

[14] ICAO Doc9303 Machine Readable Travel Documents Part 1 Machine Readable Passports Sixth Edition Volume 1, 2

[15] SUPPLEMENT to Doc9303-Part1-Sixth Edition Release 7